

I would like to state my position as a citizen on the recent inquest for comments involving wire-tapping for VoIP. I believe that forcing the internet architecture to change in order for the government to more easily wire-tap is not sound. With a court order and appropriate oversight, the government should be able to tap individuals under investigation-- but this can be accomplished by targeting the suspect's personal machine via a trojan or forensic techniques... If a suspect needs to be tapped, the government has the tools to infiltrate the person's computer and perform tapping in this manner (not unlike tapping a phone line from the residence location.) Unfortunately, the intrusiveness of the government in lobbying to change internet architecture to make VoIP wiretapping easier does not make sense. The way the internet is connected and operates does not allow for this type of individual to be targeted in a removed or remote manner without significantly hurting the free and open and efficient transport of bits over the wire. Additionally, there are encryption tools widely available which would make impossible 'listening' to a VoIP intercepted over the web once the conversation was encrypted (usually before the VoIP signal leaves the host computer). This use of encryption would only render 'listening' plausible if the suspect is targeted at the source via room bugging or as mention earlier through host machine intrusion. I strongly urge the FCC to remove themselves from this issue and every future issue involving the restructuring of the internet and IP protocol.

Thank you,

Brock J. Toon